

# HPE IceWall MFA リスクベース認証の機能と設定方法

## IceWall技術レポート



## 1 はじめに

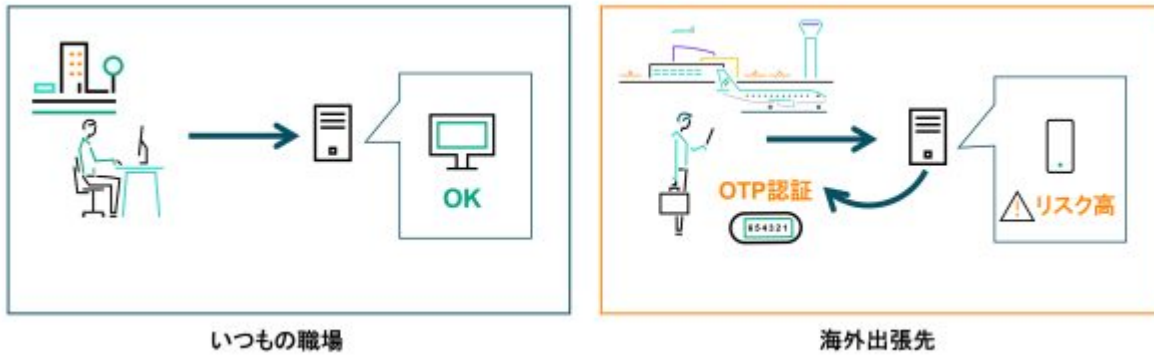
### 1.1 本技術レポートについて

本技術レポートでは、HPE IceWall MFAのリスクベース認証の機能や設定方法について説明します。

### 1.2 リスクベース認証とは

ブラウザからアクセス時に得られるデバイス情報や位置情報などをリスク分析し、その結果に応じて認証処理を実行する機能です。

海外からのアクセスなど、リスクが高いと判定された場合のみ、追加認証などを要求できます。



## 2 HPE IceWall MFAのリスクベース認証機能について

### 2.1 機能概要

HPE IceWall MFAでリスク判定を行い、その結果に応じてOTP認証などの認証方式を出し分けることが可能です。

HPE IceWall MFAで対応可能な認証方式の一覧は、[こちら](#)をご参照ください。

### 2.2 リスク判定に使用できる情報

リスク判定に使用できるクライアントの情報として、以下が利用可能です。

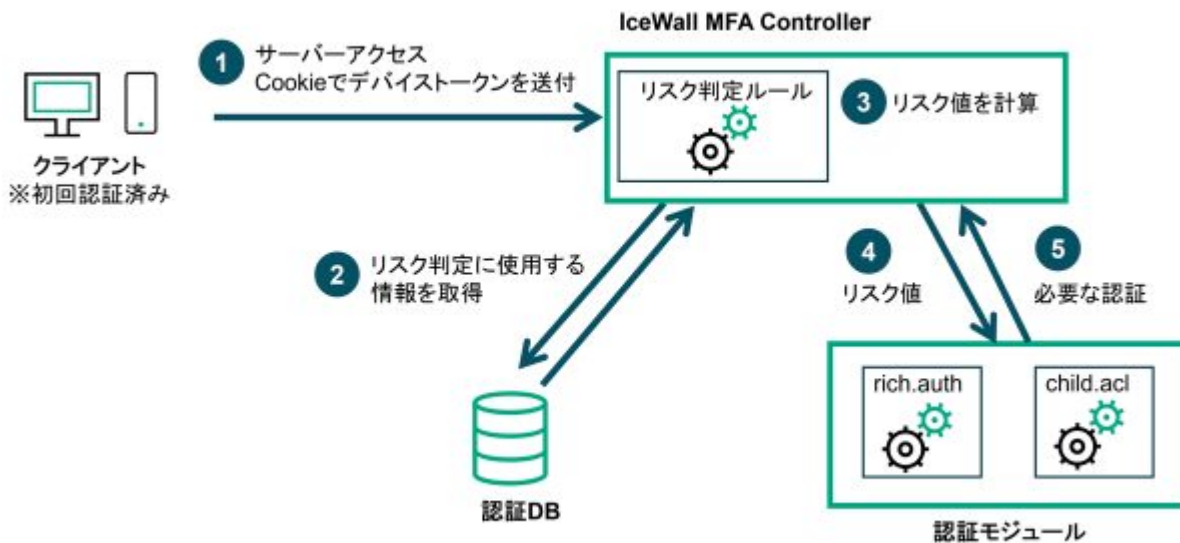
- IPアドレス値
- HTTPヘッダーのUser-Agent値から判断するOSとブラウザ種別
- その端末から初回の認証か、2回目以降の認証か
- (初回認証時にブラウザにFile Cookieで保存して確認)
- IPアドレスから取得する位置情報(国名、都市名、緯度・経度) ※1

※1：位置情報は、MaxMind社からGeolocationファイルを取得する必要があります。MaxMind社からGeolocationファイルを無料でも購読できますが、位置情報の精度が落ちます。

リスク判定に使用できる情報を利用して、以下のようなリスクベース認証が可能です。

- 海外からのアクセスは、追加認証を行う。国内からのアクセスは、追加認証を行わない。
- 指定した国以外からのアクセスは拒否する。
- 同じ端末から2回目以降の認証で前回アクセスのIPアドレスから変わっている場合、追加認証を行う。同じIPアドレスの場合は、追加認証を行わない。

## 2.3 処理の流れ



- ① クライアントからサーバーにアクセスします。クライアント端末から初回の認証時にセットしたFile Cookieがある場合は、File CookieをHPE IceWall MFAに送信します。※1
- ② 認証DBに保存されている、IPアドレス等の情報を取得します。また、認証DBに保存されている端末の識別値と、送られてきたFile Cookieの値を比較して、2回目以降のアクセスかを判断します。
- ③ クライアント端末の情報と、認証DBに保存されている値の比較などを行い、リスク値を計算します。
- ④ HPE IceWall MFAで計算したリスク値を認証モジュールに送信します。認証モジュール側で必要となる認証方式を確認します。
- ⑤ 認証モジュールからHPE IceWall MFAに必要となる認証方式を送信します。HPE IceWall MFAは、クライアント端末に対象の認証方式の画面を表示します。

※1：その端末から初回の認証の場合には、以下の画面が表示され、「登録する」ボタンを押下することでブラウザにFile Cookieが保存されます。

Risk Register Confirm

このブラウザを、普段利用するブラウザとして登録しますか。  
共有端末など、他の誰かが使う可能性のあるブラウザでは、登録しないでください。

## 3 実際の設定例

### 3.1 HPE IceWall MFA Controllerの設定例 (risk\_rule.conf)

HPE IceWall MFA Controllerの設定ファイルで、リスク値の設定を行います。

以下の設定例では「0」を低リスク（追加認証スキップ）、「1」を高リスク（追加認証が必要）としています。

設定ファイル 設定値	説明
POLICY=0,IP,EQ,10.3-255.0-255.0-255	指定したIPアドレスの場合は、リスク低とする。
POLICY=1,COUNTRY,NE,JP	日本以外からのアクセス時は、リスク高とする。
NO_TOKEN=1	認証DB内の端末を識別する値がない場合は、リスク高とする。 (いつもと違うデバイスからのアクセス)
HISTORY_IP=1	認証DB内の過去にアクセスした際のIPアドレスと一致しなかった場合は、リスク高とする。 (いつもと違うネットワークからのアクセス)
HISTORY_CITY=0	認証DB内の過去にアクセスした際の都市名と一致しなかった場合、リスク高とする。 (いつもと違う都市からのアクセス)
DEFAULT=1	すべてのルールに該当しなかった場合、リスク高とする。

### 3.2 認証モジュールの設定例 (rich.auth)

HPE IceWall MFAから認証モジュールに送られてくるリスク値によって、必要となる認証方式を判定します。

以下の設定例では「0」を低リスク（追加認証スキップ）、「1」を高リスク（追加認証が必要）としています。

設定ファイル 設定値	説明
@risk{	RICH認証名
if (RISK="0") { PW,RISK_REG	リスク値が「0」だった場合は、パスワード認証のみ行う。 認証後にデバイス登録プラグインでリスク判定に関する情報を認証DBに保存する。
} else if (RISK="1") { PW,MOTP,RISK_REG	リスク値が「1」だった場合は、パスワード認証と追加認証を行う。 認証後にデバイス登録プラグインでリスク判定に関する情報を認証DBに保存する。
} else { DENY } }	その他のリスク値だった場合は、アクセスを拒否する。

## 4 まとめ

本レポートではHPE IceWall MFAによるリスクベース認証に関するこの機能や設定方法について説明しました。

条件によって追加認証をスキップすることで、ユーザの利便性を損なわずにセキュリティを強化できます。

パスワードの漏洩などの場合にも、クライアント端末の識別値やアクセス元のIPアドレスをチェックすることで不正アクセスを防ぐことが可能となります。

ご参考：[HPE IceWall MFA リスクベース認証機能 製品概要](#)

2024.1.23 新規掲載

執筆者：日本ヒューレット・パッカーード合同会社

HPE Services統括本部 認証コンサルティング部

神原 健太

[技術レポート一覧へ →](#)

# HPE IceWall製品 お問い合わせ・資料請求

## お電話でのお問い合わせ

日本ヒューレット・パッカード カスタマー・インフォメーションセンター  
0120-268-186  
03-6743-6370 (スマートフォン・携帯電話から)

受付時間：月曜日～金曜日 9:00～19:00

(土曜日、日曜日、祝日、年末年始、および5月1日 お休み)

※ご購入後のお問い合わせは、お手元の保証書内保証規定に記載の電話番号へお問い合わせください。

## Webフォームからのお問い合わせ／製品紹介資料ダウンロード

本Webフォームよりご要望を送信いただきました方全員に、自動返信メールにて製品紹介資料ダウンロードページをご案内いたします。

[Webフォームはこちら →](#)

## HPE IceWall製品情報

[HPE IceWall トップページ →](#)

[HPE GreenLake with IceWall →](#)

[HPE IceWall MFA →](#)

[HPE IceWall SSO →](#)

[HPE IceWall Cloud Connection →](#)

[HPE IceWall Federation →](#)

[HPE IceWall 製品 オプション →](#)

[HPE IceWall 製品 動作環境 →](#)

[HPE IceWall 製品 参考価格 →](#)

[HPE IceWall 製品 サポート →](#)

[HPE IceWall 利用シーン →](#)

[HPE IceWall トピックス →](#)

## HPE IceWall関連資料

[技術レポート →](#)

[お客様事例 →](#)

[製品・お客様事例カタログ →](#)

[トレーニングコース →](#)

## HPE IceWall関連情報

[IceWall パートナー一覧 →](#)

[認証・シングルサインオン用語集 →](#)

[HPE Blog, Japanアカウント : IceWall\\_Mktg →](#)

## HPE IceWall お問い合わせ

[よくあるご質問 →](#)

[お電話でのお問い合わせ・資料請求 →](#)

[Webフォームからのお問い合わせ・資料請求 →](#)

[HPE IceWallクラウドデモのお申し込み →](#)

## 関連製品

[HPE Quarantine System →](#)

# お探しの情報は見つかりましたか？



ご購入方法



製品サポート



営業へのお問い合わせ



お問い合わせ先一覧



## 企業情報



会社情報

アクセス

お問い合わせ

採用情報

HPEについて

インクルージョン & ダイバーシティ

サステナビリティと企業責任

経営幹部

## お知らせ



ニュースルーム

イベント・セミナー

新着情報

重要なお知らせ

## パートナー



パートナープログラム

認定資格制度

OEMソリューション



---

## サポート



製品サポート

ソフトウェア & ドライバー

標準保証確認

オペレーショナルサポート

教育とトレーニング

製品リサイクル

機器部品の妥当性確認

---

## コミュニティ



HPE Japan ブログ

---

## リソース



お客様事例

ご購入方法

オンラインストア

HPE Customer Center

Eメール登録


ドキュメントライブラリ

Resource Library

ビデオギャラリー

金融サービス

---

 日本 (ja)

© Copyright 2024 Hewlett Packard Enterprise Development LP

[個人情報保護方針](#) | [ご利用条件](#)・[免責事項](#) | [AdChoices & クッキー](#) | [サイトマップ](#)

